UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Office and attached space of Watry Homes, LLC, located in a commercial building found at 17790 West Liberty Lane, New Berlin, Wisconsin

Case No. 13-M-562

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Office and attached space of Watry Homes, LLC, located in a commercial building found at 17790 West Liberty Lane, New Berlin, Wisconsin

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. Sections 1001, 1012, 1341 and 1343	False statements, false statements to HUD, mail fraud and wire fraud.

The application is based on these facts:
See attached affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

John Klugiewicz, FBI Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: October 15, 2013 at 1:50 PM

Judge's signature

City and state: Milwaukee, Wisconsin

Hon. William E. Callahan, Jr., Magistrate Judge
Printed name and title

AFFIDAVIT

John Klugiewicz, being first duly sworn on oath, hereby deposes and says:

Introduction and Agent Background

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been so employed for 27 years. I am currently assigned to the Milwaukee Division's White Collar Crime Squad. As part of my duties, I investigate violations of federal criminal laws.

2. During my 27 years as a FBI Special Agent, I have participated in:

a. Numerous fraud investigations, warrants, and seizures;

b. The execution of numerous search warrants for documents, records and proceeds from illegal activities, including searches of offices of business entities involved in illegal activity;

c. The subsequent investigations and analyses of evidence seized pursuant to those warrants; and

d. The interviewing of individuals who may have had personal knowledge of the illegal activities under investigation.

3. This affidavit is submitted in support of an application for a search warrant for evidence of violations of 18 U.S.C. §§ 1001, 1012, 1341, and 1343.

4. The search warrant applied for is to search for items set forth in Attachment A which are currently on the premises located at Watry Homes, LLC, an office and attached space located at 17790 West Liberty Lane in New Berlin, Wisconsin.

5. The facts set forth in this affidavit are based on my own personal knowledge from participating in the investigation of this matter; knowledge that I have obtained from other people involved in the investigation including investigators from the United States Department

of Housing and Urban Development (HUD) and United States Department of Labor (DOL); interviews of witnesses; my review of records related to this investigation; and knowledge gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause to support an application for a search warrant, it does not set forth each and every fact that has been obtained during the course of this investigation.

Summary of Relevant Information

6. The United States is investigating Scott Watry and his company, Watry Homes, LLC for the alleged submission of fraudulent claims to HUD and the alleged submission of fraudulent documents to DOL in connection with the work of Watry Homes on the Westlawn public housing project in Milwaukee. In 2011, Watry Homes was a successful bidder on several subcontracts to install roofing and siding as part of the Westlawn project. The Westlawn project consisted of the demolition of 332 existing public housing units and the construction of 250 new affordable housing units in the city of Milwaukee in the vicinity of 60th Street and Silver Spring Drive. Construction of the Westlawn project began in 2011 and was completed in late 2012.

7. Financing for the construction of the Westlawn project included approximately $12.3 million provided by HUD, subject to various federal legal requirements and conditions. Because the Westlawn project received this federal financing, the federal Davis-Bacon Act requires all contractors and subcontractors who worked on the Westlawn project to pay laborers employed on that project at or above the locally prevailing wages, including fringe benefits, as determined in the contract's Davis-Bacon wage determination. 40 U.S.C. §§ 3141-3144. For the Westlawn project, the Davis-Bacon wage was determined to be approximately $45 per hour for a carpenter/sider and approximately $42.50 per hour for a roofer. Contractors and subcontractors

are required to pay covered workers weekly and to submit weekly certified payroll records to the contracting agency.

8. In regard to that requirement, Watry Homes was required to submit a weekly certified payroll report listing its workers who worked on the Westlawn project during that week, the number of hours worked by each of those employees, and the wage rate per hour paid to each employee. The certified payroll reports submitted by Watry Homes on the Westlawn project have been obtained as part of this investigation and reflect that Watry Homes always reported that it was paying legally required hourly wages to its workers.

9. Mary Stoecker, a contract compliance officer for the Housing Authority of the City of Milwaukee (HACM), was interviewed about the Westlawn project and Watry Homes. She stated that Scott Watry, the owner and operator of Watry Homes, originally submitted a contract wage rate sheet saying that Watry Homes would pay siders $16 per hour. Ms. Stoecker states that she wrote "No" on that contract wage rate sheet and sent Scott Watry an email telling him that he could not pay $16 per hour but would be obligated to pay the prevailing Davis-Bacon wage rate on the Westlawn project.

10. Altius Construction was a contractor on the Westlawn project for which Watry Homes was a subcontractor. Mary McLeod, a secretary at Altius, was interviewed as part of this investigation. Ms. McLeod recalled that after the Westlawn contracts were awarded she discussed the Davis-Bacon prevailing wage requirements with Scott Watry. She also stated that Mr. Watry was required to certify to Altius that he understood and would adhere to Davis-Bacon wage requirements. She also stated that Mr. Watry was made aware of the Westlawn Davis-Bacon wage requirements on several other occasions including being provided with written and oral instructions regarding those requirements.

11. Ms. McLeod also stated that Mr. Watry was present at an all-subcontractor meeting called by Prism, a consultant hired by construction manager Hunzinger Construction to provide guidance and oversight with regard to Davis-Bacon wage requirements. At that meeting, Prism provided additional information on Davis-Bacon wage requirements.

12. A woman named Heather Ramos approached me in April, 2013 and has stated the following in several interviews regarding her dealings with Scott Watry and Watry Homes.

a. Ms. Ramos operates a roofing company incorporated as R&R Exteriors, LLC which supplies laborers to install roofs. R&R frequently worked with Scott Watry, the president of Watry Homes, from 2008 through 2012. Watry Homes would obtain contracts for roofing projects, supply the materials for those projects, and subcontract with R&R for the installation of the roofs.

b. Ms. Ramos is an acquaintance of Jose Luis Campos Flores who is also experienced in roofing work. In approximately 2009, Ms. Ramos began to use Mr. Campos Flores and his roofing crew on various projects. Mr. Campos Flores eventually incorporated his business under the name Exterior Services, LLC. Ms. Ramos states that many of Mr. Campos Flores' workers were aliens lacking authorization to work in the United States.

c. In 2011, Watry Homes, LLC won a subcontract to install roofs and siding for the Westlawn project. According to Ms. Ramos, Scott Watry led a scheme to fabricate employee identities and payroll to make it appear that he was paying Davis-Bacon wages to Watry Homes' employees when, in fact, others were actually performing the work on the Westlawn project for far less pay. To accomplish this scheme, Mr. Watry asked Ms. Ramos to provide identification documents for individuals authorized to work in the United States who Mr. Watry would then represent as laborers to whom he was paying Davis-Bacon wages. Ms. Ramos

admits that she provided Mr. Watry with documents to establish four such identities, her own, Mr. Campos Flores, Dulce Garcia who is the mother of Mr. Campos Flores' children, and Alibert Garrido. A similar request was made by Mr. Watry to Mr. Flores Campos and Ms. Ramos witnessed Mr. Campos Flores purchasing fraudulent identification documents to provide to Mr. Watry.

d. Ms. Ramos states that the fraudulent scheme was pursued by fabricating payroll checks and information during 2011 and 2012 when the roofing and siding was being installed in the Westlawn project. During that time, Watry Homes would issue fraudulent payroll checks made out to the four identities that Ms. Ramos had given Mr. Watry as though those four individuals were employees of Watry Homes. These payroll checks and check stubs falsely represented payment of Davis-Bacon wages, but for far fewer hours than were actually worked by the actual laborers. Ms. Ramos would deposit these false payroll checks into the R&R Exteriors' bank account. She would then pay the funds to Mr. Campos Flores, whose crew had actually performed the work. Ms. Ramos provided some bank records and invoices which corroborated her statements.

e. Ms. Ramos advised that neither she, Dulce Garcia, nor Alibert Garrido actually worked on the Westlawn project but their names were listed on the weekly payroll certifications submitted by Watry Homes and she received payroll checks for herself as well as Garcia and Garrido from Watry Homes. Ms. Ramos advised that the checks written to her, Ms. Garcia, and Mr. Garrido were all deposited by her into her R&R Exteriors' account and then she wrote out checks to Mr. Campos Flores who would pay the actual workers.

f. Ms. Ramos indicated that the complete records of the bank accounts involved would substantiate her allegations of how the money went from Watry to her to Campos Flores. These records have been obtained and do substantiate Ms. Ramos' description.

g. Ms. Ramos stated that Watry Homes engaged in similar schemes to conceal its failure to pay Davis-Bacon wages on subcontracts for other federally financed projects to repair houses controlled by the housing authorities for the Wisconsin cities of Waukesha and Beloit.

13. In this way, Mr. Watry was able to create records indicating that the work had been done by certain people being paid Davis-Bacon wages for fewer hours when, in fact, the work was done by other people being paid lower hourly wages but working more hours.

14. Before Ms. Ramos approached me, investigators from the DOL Wage and Hour Division had separately commenced an investigation of Watry Homes concerning potential Davis-Bacon Act violations. Emails sent by Mr. Watry to DOL investigators establish that Mr. Watry represented to the investigators that the laborers installing the roofs and siding at the Westlawn project were employees of Watry Homes.

15. On August 29, 2012, Scott Watry spoke with the DOL Wage and Hour investigator. Mr. Watry stated that all of his employees on the Westlawn project were paid for all the hours they worked at the Davis-Bacon prevailing wage rates which were $45 or $42.50 per hour. Mr. Watry said that this was true but then stated that he would not sign the written statement to that effect that the investigator prepared.

16. Various other workers on the Westlawn project were interviewed by the DOL Wage and Hour Division about their work on behalf of Watry Homes on the Westlawn project.

They worked as carpenters, roofers, and siders. They also consistently alleged the following Davis-Bacon violations:

- During the periods of time they worked for Watry Homes on the Westlawn Project, these workers generally worked full time on the project, 40 hours or more per week.
- They were paid at hourly wage rates generally approximately $20 per hour but the wage rates they reported ranged anywhere from $10 to $27 per hour.
- However, the check stubs they received when they were paid by Watry Homes reflected that they were actually paid $42 to $45 per hour for working many fewer hours than they had actually worked.
- Although these check stubs were inaccurate and some of them understood that they were supposed to be paid at higher rates per hour, these workers did not complain because they feared they would lose their jobs if they did.
- A number of these workers reported that Scott Watry or other supervisors from Watry Homes told them to sign false payroll reports and to not be truthful with any government investigators who contacted them about their rates of pay and number of hours worked.

17. In my investigator experience, I have consistently found that business entities maintain records including employee information, payroll information, contract information, and banking records in their offices. The records normally found in a search in a business office include paper documents as well as records kept on computer systems used by that office.

18. According to records maintained by the Wisconsin Secretary of State's office, Watry Homes, LLC was incorporated in Wisconsin on April 13, 2001. The registered agent is listed as Scott R. Watry, 17790 West Liberty Lane, New Berlin, Wisconsin 53146. That is not Mr. Watry's home address but is the address of the office for Watry Homes.

19. As part of DOL's wage and hour investigation, Traci Jensen was interviewed. Ms. Jensen advised that she is Scott Watry's assistant at the Watry Homes' office and has been employed in that position since early 2012. She states that she prepares and maintains payroll records based on timesheets submitted to her by Mr. Watry.

20. The Wage and Hour investigator from DOL interviewed both Mr. Watry and Ms. Jensen at the Watry Homes' office on Liberty Lane in New Berlin, Wisconsin. The DOL investigator described the office as having computers and desks and file cabinets. She stated that Ms. Jensen retrieved requested materials from cabinets there.

21. Nicholas Oberdorf is a construction worker who has worked for Watry Homes on various projects in the past. He was interviewed as part of this investigation. Mr. Oberdorf has stated that he was last inside Watry Homes' office on September 23, 2013. He states that Ms. Jensen was there at her desk with a computer and file cabinets. Scott Watry was in his office with a desktop computer.

22. I have also spoken to an Occupational Safety and Health Administration investigator who was present in the Watry Homes' office on May 22, 2013. That investigator reported that the premises included a secretary's office, a conference room, and Mr. Watry's office. He stated that the premises included a storage area, desktop computers, and file cabinets.

23. Heather Ramos made various statements about records created and stored at the Watry Homes' office in New Berlin. Ms. Ramos recalled working with Ms. Jensen to create spreadsheets of payroll by employee for various jobs. Ms. Ramos stated that the identifying information she provided to Mr. Watry for him to use to identify certain individuals as Watry Homes' workers was maintained in black file cabinets in the Watry Homes' office.

Search and Seizure of Computer/Electronic/Digital Data

24. This application seeks permission to search for and seize evidence of the crimes described above stored on computers and electronic/digital devices (collectively, "digital devices"), as well as any digital devises that constitute instrumentalities of the crimes.

25. I have spoken with Special Agent Matthew Petersen who has training in the forensic examination of computers and digital devices and is a Field Examiner in the Milwaukee office. SA Petersen related various information to me and/or confirmed various information for me as noted below.

26. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices including SA Petersen, I know that data in digital form can be stored on a variety of systems, storage devices, or media including hard disk drives, floppy disks, compact disks, magnetic tapes, flash drives, and memory chips. Some of these devices can be smaller than a thumbnail and can take several forms, including thumb drives, secure digital media used in phones and cameras, personal music devices, and similar items.

27. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices including SA Petersen, I know that computers and digital devices are often used to store information, very much the same way paper, ledgers, files and file cabinets are used to store information. I know that it is common today for businesses to utilize computers to conduct their business and to store information related thereto. I also know that it is common for individuals to have personal computers and to use these computers to conduct their personal affairs, their business affairs, and to store information related thereto. I know based on my training and experience, including prior

investigations specifically related to the investigation of Watry, that subjects who are engaged in fraud commonly store information related to their activities on computers and digital devices.

Removal of Data Storage Devices For Review In A Laboratory Setting May Be Required

28. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices including SA Petersen, I know that a forensic image is an exact physical copy of a data storage device. A forensic image captures all data on the subject media without viewing or changing the data in any way. Absent unusual circumstances, it is essential that a forensic image be obtained prior to conducting any search of data for information subject to seizure pursuant to the warrant. I also know that during the search of the premises it is not always possible to create a forensic image of or search digital devices or media for data. I also know that it is frequently necessary to remove digital devices or media for later laboratory evaluation off-site under controlled circumstances. This is true for a number of reasons, including the following:

a. Searching digital devices can be a highly technical process that requires specific expertise and specialized equipment. Because there are so many different types of digital devices and software in use today, it is difficult to anticipate all of the necessary technical manuals, specialized equipment, and specific expertise necessary to conduct a thorough search of the media to ensure that the data will be preserved and evaluated in a useful manner.

b. Searching digital devices can require the use of precise, scientific procedures designed to maintain the integrity of the evidence. The recovery of such data may require the use of special software and procedures, such as those used in a law enforcement laboratory.

c. The volume of data stored on many digital devices is typically so large that it will be highly impractical to search for data during the execution of the physical search of the premises. Storage devices capable of storing 500 gigabytes of data are now commonplace in desktop computers. It can take several hours, or even days, to image a single hard drive. The larger the drive, the longer it takes. Depending upon the number and size of the devices, the length of time that agents must remain onsite to image and examine digital devices can become impractical.

d. Since digital data may be vulnerable to inadvertent modification or destruction, a controlled environment, such as a law enforcement laboratory, may be essential to conduct a complete and accurate analysis of the digital devices from which the data will be extracted. Software used in a laboratory setting can often reveal the true nature of data. Moreover, a computer forensic reviewer needs a substantial amount of time to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband, or an instrumentality of a crime.

e. Analyzing the contents of a computer or other electronic storage device, even without significant technical difficulties, can be very challenging, and a variety of search and analytical methods must be used. For example, searching by keywords, which is a limited text-based search, often yields thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process. The computer may have stored information about the data at issue which may not be searchable text, such as: who created it; when and how it was created, downloaded, or copied; when it was last accessed; when it was last modified; when it was last printed; and when it was deleted. The relevance of this kind of

data is often contextual. Furthermore, many common email, database, and spreadsheet applications do not store data as searchable text, thereby necessitating additional search procedures. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed data requires a search of events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which users logged in, whether users shared passwords, whether a computer was connected to other computers or networks, and whether the users accessed or used other programs or services in the relevant time period, can help determine who was sitting at the keyboard.

f. Searching digital devices can require the use of precise, scientific procedures designed to recover latent data. The recovery of such data may require the use of special software and procedures. Data that represents electronic files or remnants of such files can be recovered months or even years after it has been downloaded onto a hard drive, deleted, or viewed via the Internet. Even when such files have been deleted, data can be recovered months or years later using readily available forensic tools. Normally, when a person deletes a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in space on the hard drive or other storage media that is not allocated to an active file. In addition, a computer's operating system may keep a record of deleted data in a swap or recovery file or in a program specifically designed to restore the computer's settings in the event of a system failure.

29. This warrant seeks authority to seize contextual data, that is, evidence of how a digital device has been used, what it has been used for and who has used it. It can be very

important in criminal cases to seek "attribution" data so that an event or communication can be associated with a person. Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices including SA Petersen, this authority is sought for a number of reasons:

a. In some instances, the computer "writes" to storage media without the specific knowledge or permission of the user. Generally, data or files that have been received via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to such data or files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve artifacts of electronic activity from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer usage. Logs of access to websites, file management/transfer programs, firewall permissions, and other data assist the examiner and investigators in creating a "picture" of what the computer was doing and how it was being used during the relevant time in question. Given the interrelationships of the data to various parts of the computer's operation, this information cannot be easily segregated.

b. Digital data on the hard drive that is not currently associated with any file may reveal evidence of a file that was once on the hard drive but has since been deleted or edited, or it could reveal a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave digital data on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, email programs, and chat programs store configuration data on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional

data, such as the attachment of peripherals, the attachment of USB flash storage devices, and times the computer was in use. Computer file systems can record data about the dates files were created and the sequence in which they were created. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations (or on other devices).

c. Further, evidence of how a digital device has been used, what it has been used for, and who has used it, may be learned from the absence of particular data on a digital device. Specifically, the lack of computer security software, virus protection, malicious software, evidence of remote control by another computer system, or other programs or software may assist in identifying the user indirectly and may provide evidence excluding other causes for the presence or absence of the items sought by this application. Additionally, since computer drives may store artifacts from the installation of software that is no longer active, evidence of the historical presence of the kind of software and data described may have special significance in establishing timelines of usage, confirming the identification of certain users, establishing a point of reference for usage and, in some cases, assisting in the identification of certain users. This data can be evidence of a crime, can indicate the identity of the user of the digital device, or can point toward the existence of evidence in other locations. Evidence of the absence of particular data on the drive is not generally capable of being segregated from the rest of the data on the drive.

Search Procedure

30. Watry Homes is a functioning company that conducts legitimate business. The seizure of the company's computers may limit the company's ability to conduct its legitimate business. As with any search warrant, I expect that this warrant will be executed reasonably.

Reasonable execution will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, officers will copy data, rather than physically seizing computers, to reduce the extent of disruption. If employees of the company so request, the agents will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of the company's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

Data to be Seized

31 Based upon my training and experience, and information related to me by agents and others involved in the forensic examination of computers and digital devices, I know that, in order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize, image, copy, and/or search the following items, subject to the procedures set forth herein:

a. Any computer equipment or digital devices that are capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence of such crimes, as set forth in Attachment A;

b. Any computer equipment or digital devices used to facilitate the transmission, creation, display, encoding, or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners that are capable of being used to commit or further the crimes outlined above, or to create, access, process, or store evidence of such crimes, as set forth in Attachment A;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, personal digital assistants, and cell phones capable of being used to commit or further the crimes outlined above, or to create, access, or store evidence of such crimes, as set forth in Attachment A;

d. Any documentation, operating logs, and reference manuals regarding the operation of the computer equipment, storage devices, or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles, or similar physical items which are necessary to gain access to the computer equipment, storage devices, or data;

g. Any passwords, password files, test keys, encryption codes, or other information necessary to access the computer equipment, storage devices, or data; and

h. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show the actual user(s) of the computers or digital devices during any time period in which the device was used to commit the crimes referenced above, including the web browser's history; temporary Internet files; cookies, bookmarked, or favorite web pages; email addresses used from the computer; MAC IDs and/or Internet Protocol addresses used by the computer; email, instant messages, and other electronic communications; address books; contact lists; records of social networking and online service usage; and software that would allow others to

control the digital device such as viruses, Trojan horses, and other forms of malicious software (or alternatively, the lack of software that would allow others to control the digital device).

i. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the computer or digital device.

j. All records, documents, programs, applications, or materials created, modified, or stored in any form, including in digital form, on any computer or digital device, that show contextual information necessary to understand the evidence, contraband, fruits, or instrumentalities described in this attachment.

Retention of Image

32. The government will retain a forensic image of each digital device subjected to analysis for a number of reasons, including proving the authenticity of evidence to be used at trial; responding to any potential questions regarding the corruption of data; establishing the chain of custody of data; refuting any potential claims of fabrication, tampering, or destruction with/of data; and addressing potential exculpatory evidence claims where, for example, a defendant claims that the government avoided its obligations by destroying data or returning it to a third party.

Inventory and Return

33. With respect to the seizure of electronic storage media or the seizure or imaging of electronically stored information, the search warrant return to the Court will describe the physical storage media that were seized or imaged.

ATTACHMENT A

Any and all documents in whatever form, relating to Watry Homes, LLC's work on federally-financed construction projects including the Westlawn project. These documents include, but are not limited to, contracts, explanations relating to the payment of legally required wage rates, employees working on these projects, the identifying information for these employees, wages paid on these projects, hours worked on these projects, and functions performed by the workers identified.